Quality Assurance Criteria 2015–18

Enhanced guidance on meeting quality assurance criterion 4.5

Assessment materials and candidate evidence (including examination question papers, scripts and electronically stored evidence) must be stored and transported securely.

This edition: March 2018
Publication code: CA7202D

Published by the Scottish Qualifications Authority
The Optima Building, 58 Robertson Street, Glasgow G2 8DQ
Lowden, 24 Wester Shawfair, Dalkeith, EH22 1FD
www.sqa.org.uk

Introduction to your procedures

This criterion relates primarily to assessments where a candidate would gain an unfair advantage by seeing the assessment in advance when the assessment is carried out under controlled conditions.

These could be:

- assessments produced by SQA and published on the SQA secure site
- assessments produced within the centre

Centres which offer qualifications requiring assessments to be stored securely must have a documented procedure for the management of this.

This could be:

- a stand-alone procedure
- part of an assessment policy and procedure
- part of a wider security of assessment procedure, also covering external assessment

Your procedures should cover:

- centre managers and staff taking sufficient steps to protect the integrity of SQA assessments before and after assessment takes place (see detail below)
- allocating responsibility for management of security of assessments
- making security of assessments everyone's responsibility
- methods of storage (electronic, hard copy)
- reviewing your existing procedures regularly
- how all relevant staff are aware of these procedures (including covering in induction)
- providing access to secure storage arrangements for SQA staff, for QA purposes

Access to SQA's secure site

Your SQA Co-ordinator will have been given a secure log-in to SQA's secure site, if you deliver qualifications with published assessment exemplars.

You must decide on your approach to use of the secure log-in, for example:

- Only the SQA Co-ordinator has access and downloads assessment exemplars for teaching staff/assessors on request
- Other members of the quality team/administrative staff have access, in addition to the SQA Co-ordinator and they download assessment exemplars for teaching staff/assessors on request

- Other identified individuals are given the log-in details (eg heads of department, managers, administrators) so that they can browse the secure site and download assessments themselves

If other members of staff are given the secure log-in you must consider:

- How do you decide who gets access?
- How and where do you record this?
- How will you ensure that these members of staff understand the security requirements?
- What is the procedure if one of these members of staff leaves?
- How will you make all staff aware that any breach in the security of the assessment materials published on the secure site must be reported immediately to SQA via your SQA Co-ordinator.
- How often will you change the password? Who will do this? How will you inform the other members of staff who have access to the log-in?

Once assessments have been downloaded from the secure site, you must consider the following issues and make all relevant staff aware of your approach:

- If sending electronically, how will this be done securely (eg encrypted e-mail, secure area of VLE or intranet)?
- If a teacher/assessor is downloading them directly, where will they store them (eg encrypted memory stick, personal drive, secure area of VLE or intranet)?
- If they are printed off, how will they be passed and stored securely (eg secure internal mail, put into locked cabinets rather than being left on a desk)?
- How will they be accessed by staff to be used for assessments, and what will be done with them after the assessment?

Secure storage to and access to internally-devised assessments

The same principles apply to access to and storage of internally-devised assessments as to assessments published by the SQA.

If these are held electronically:

- Where are they held (eg shared drive, intranet, VLE)?
- How is security protected (eg password log-in)?
- Who has access and who decides this?

If these are held in hard copy:

- Where are they held (eg centrally with quality team, in administrative offices, in staff work areas)?

- How is security protected (eg locked cabinets, limited access to keys)?
- Who has access and who decides this?

Transport

Transport arrangements within and between assessment sites, or between a central base and an assessment site, must also ensure the security of the materials.

Assessments in use

All staff using assessments which are stored securely with candidates, must be made aware of the following requirements on them:

- The assessments must not be left lying in classrooms, or work rooms
- Assessments handed out to candidates to use must be collected back in and either shredded, put into confidential waste or stored securely again (this would include assessment papers or booklets with the questions embedded in them)
- All candidates must be made aware that taking away assessments, copies or images of assessments is malpractice, and could result in a disciplinary process
- Staff who give assessments, copies or images of assessments to candidates outwith the assessment process, without good reason or permission, are committing malpractice, which could result in a disciplinary process
- Any breaches of security of assessment must be reported immediately to the SQA Co-ordinator or relevant manager

Candidate assessment evidence

Assessment evidence produced by candidates must also be held and moved securely. This is to ensure that the interests of the candidates are protected and to protect the integrity of the assessment by ensuring that the evidence cannot be tampered with.

In all circumstances, where electronic evidence is being used, centres must ensure the evidence submitted by candidates:

- is received securely by the appropriate designated centre staff
- cannot be altered by others — candidates must be able to protect/lock their evidence before they submit it
- is stored securely in a restricted access file throughout assessment and until the completion of the assessment and quality assurance processes

Electronic assessment evidence should ideally be submitted by the candidate and held securely using eg e-portfolios or VLEs. If it has to be submitted in another way (eg by e-mail or on memory stick), it should be protected (eg encrypted, locked with password access).

Assessors and internal verifiers accessing electronic assessment evidence, including for quality assurance purposes, should use a form of remote signature. As with conventional signatures, assessors and verifiers must be able to signify in a legitimate way that they have confirmed assessment/verification decisions. This could be done by the assessor/verifier using a code — ie using an appropriate password, PIN, electronic signature or symbol, or any combination of these. Whatever code is used, it must be secure and only be available for use by the assessor or verifier it belongs to, just as a hand-written signature would be.

SQA requires centres to retain all candidate evidence for the Group Award/Units until at least three weeks after the official completion date (the completion date provided to SQA). However, if the first contact for the session is made by the Qualification Verifier before three weeks after the completion date, all candidate evidence must be retained until after the verification visit has taken place.

You must establish how you will give secure access to electronically-held candidate evidence to SQA external verifiers. The external verifier may request access to the evidence prior to the visit, in which case they will ask you provide them with secure access. This could be by providing them with an ID and password for an agreed period of time. You may need to provide help to the external verifier with navigational/functional issues if required.

Suitable arrangements should also be made to ensure that candidate assessment evidence in hard copy format is submitted, moved and stored securely.